The UK Access Management Federation
FOR EDUCATION AND RESEARCH

COVENTRY UNIVERSITY

Colin Bruce

Table of Contents

These case studies, prepared by organisations who participated in the JANET Shibboleth on Windows project, are provided for information purposes only and reflect the particular arrangements and experience of those concerned. In each case, the configuration, installation and implementation of the Shibboleth on Windows software will vary according to the type of infrastructure and technical resources involved.

Executive Summary

This case study describes the deployment experiences of the Shibboleth on Windows group at Coventry University. The team deployed Shibboleth on Windows Server 2003 and Windows Server 2008 running on a virtual server. The work was undertaken as part of JANET(UK)'s Shibboleth on Windows[1] project.

Background Information

About the organisation

Coventry University is a post-1992 University with approximately 17,000 students, mostly undergraduate, and 2,500 staff. The University makes extensive use of on-line learning systems.

[1] *http://www.ja.net/development/middleware/shibboleth-on-windows.html*

Resources

Three staff worked in the evaluation on a part-time basis. None had any significant experience of Shibboleth before this project started. The University infrastructure is predominately a Microsoft Windows Server 2003 environment.

Current situation

Access to external sources is controlled using a mixture of classic ATHENS and IP address ranges.

Access Management

Had you used any other forms of Access Management previously?

> Yes. We have used ATHENS for many years as the main access management system for access to remote resources. However, some resources are accessible from any system within our IP address range.

What were the drivers for deploying Federated Access Management?

> The demise of classic ATHENS as a 'free' resource and the benefits that a world-wide service brings.

What services do you want to be federated?

> Internal and external services.

Are you working towards single sign-on?

> There is a current Business Plan objective to provide single sign-on and it is believed that Shibboleth may help with this. Currently only external resources are federated but the University is a major user of WebCT VISTA and is investigating Moodle, both of which are candidates for shibbolising (i.e. making compatible with Shibboleth).

Aims and Objectives

The immediate purpose of this work was to test and evaluate the installer package. However, in this particular case the work was carried out on two operating systems running in a virtual environment using VMWare.

Methodology

Two virtual servers were built using VMWare. The first used Microsoft Windows Server 2003 as its operating system and the second used Microsoft Windows Server 2008. The usual VMWare facilities such as VMotion and Dynamic Resource Scheduling were tested. All the work was carried out in-house. The LDAP requirements were met by the University Active Directory infrastructure.

The virtual server running Windows Server 2003 was configured as follows:

CPU	2
Memory	2048MB
Disk	10GB
Network	1Gbit/s

The server running Windows Server 2008 had the same configuration but with a 16GB disk instead of a 10GB disk. Both servers were hardened using the Microsoft Security and Configuration Wizard.

Two servers running VMWare ESX version 3.5 were used to host these and other servers. They were both the same and were configured with:

CPU	2 x dual core 2GHz Xeon
Memory	32GB
Disk	378GB
Network	4 x 1Gbit/s

Implementation

Who was involved in the process within your organisation?

Three members of staff from the IT Services department in Coventry University.

What were your objectives for deploying Federated Access Management?

To test the Shibboleth on Windows installer in various configurations.

What were your experiences – what went well, what were the main challenges and how did you overcome them?

Installation of Shibboleth on Windows 2003 and 2008 was very straightforward. The university operates a single domain, single forest infrastructure so there were no cross-domain issues to deal with. Integration with the existing Windows infrastructure was easy as the installer did virtually the entire configuration necessary. However, if a UNIX-based LDAP service was being used instead of Active Directory then some of the settings would have to be changed. The main setting that would be affected would be 'Search filter' in resolver.xml where UID would have to be used instead of sAMAccountName. However, some third party LDAP servers may use different attributes.

How long did it take?

The overall project has run for around 6 months. However, staff have only worked on it on a part-time basis. The general view is that with sufficient knowledge the Identity Provider could be installed and configured in a few hours.

What were your training/support and roll-out experiences? How was this done/evaluated?

We did not undertake any formal training although some people attended JISC seminars and the presentation given by Rod Widdowson and the associated material given out at that meeting proved to be very useful.

There was a minor difficulty with the early version of the installer where the uninstall option didn't seem to work. However, it had and by the time the problem had been noted a new version of the installer was available and the issue was never seen again. Although the older version was reinstalled later the uninstall option worked so it was not investigated further.

The initial install was very easy and the system worked straight away. Others have reported configuration difficulties with more complex LDAP set-ups than Coventry University. However, we have a very simple single forest/single domain arrangement so we didn't have any problems with the initial install.

Making it work with Service Providers is somewhat harder since that often requires modification of configuration files which are XML files. This is not an issue with the installer but is the way Shibboleth has been written. However, our experiences with that aspect of the installation may be of some use to others starting out with Shibboleth.

Do you have any hints/tips/gotchas to look out for and things you would do differently?

We changed some of the configuration files to meet the requirements of various Service Providers. We then had to hide some of these configuration changes from EduServ by adjusting Attribute Release Policies. EduServ is required for those Service Providers that have not yet converted to a federated identity management system. Although these issues are not to do with the installer and nothing we did is particularly complex, some of the information may be useful to others and so has been included in the 'Best Practice Guidance' document (see Appendix).

There are some user level and technical suggestions which may be of interest to people deploying Shibboleth on Windows for the first time which have also been included in the 'Best Practice Guidance' document.

Use forms based authentication and customize the login page to meet the requirements set by the Library. The Shibboleth on Windows installer implements forms-based authentication but the page needs to be modified. More information on this is provided in the 'Best Practice Guidance' document.

Involve colleagues from the organisation's Library (who are usually responsible for access to remote resources).

Use the JANET test sites and the JANET Help Desk when stuck. There is more about this in the 'Best Practice Guidance' document.

Consider using a virtual server to implement Shibboleth. Installation is the same as it would be if it were installed on a physical server but there are many benefits to virtualising such as reduced power consumption and high availability.

What have been the actual benefits since deployment – improvements in end user experience; administration; convergence of internal/external systems. etc.

> User management and administration is much simpler in a Shibboleth environment compared to the classic ATHENS system since it is linked to the University Active Directory system. However, this brings its own set of problems. For example, the University Library has requested that we provide a system that allows them to prevent people from accessing Shibboleth protected resources without blocking them from using other resources controlled by Active Directory. We have not been able to do this yet although a method of achieving it has been devised. Again this is not an issue with the installer but may be of interest to those deploying Shibboleth using the installer.

Are there any aspects of the process of deployment that could be made easier with centralised effort (i.e. JANET assistance)?

> The deployment was very simple and the installation procedure is very clear so that aspect probably does not need any further assistance. However, as use of Shibboleth grows many institutions will want to configure it to do other things such as being able to block individuals or shibbolize internal services, and it may be that JANET could provide some assistance there if demand was sufficient.

Project Experience

From our point of view the project went very well although much of the work seemed to coincide with holidays and busy periods at Coventry University. The mixture of face to face meetings and online meetings was welcome. The input from the developer of the installer was very useful.

Conclusions and Implications

The Shibboleth installer works very well and is clear, simple and reliable. Full deployment of Shibboleth requires quite a bit of configuration once the installer has done its job.

Recommendations

1. *Deploy in a virtual environment using one of the virtualisation systems that provides the ability to move running virtual servers seamlessly from one host server to another; for example Xen.*

2. *Read the introductory pages on the Internet2 and UK Federation web sites.*

3. *Understand how Shibboleth works. The UK Federation have provided some information on this.*

References

Virtualisation Using Xen:
http://xen.org

Introductory Pages:
http://shibboleth.internet2.edu/
http://www.ukfederation.org.uk/

How Shibboleth Works:
http://www.ukfederation.org.uk/content/Documents/HowItWorks

Appendix: Shibboleth Best Practice Guide – Guidance for Installing and Running Shibboleth on Windows

Introduction

This document provides some information that is intended to help those installing, configuring and testing Shibboleth on a Windows server. It is not an installation, configuration or testing guide – there are other documents that provide such information. Instead it is a document which provides additional information that may compliment these guides

Installation

Research

When deploying new hardware or software it is tempting to put the CDROM in a server and run setup. The installer is quick and easy to use. However, once Shibboleth is installed some configuration is required. This will be much easier if those carrying out the installation know and understand the terminology. Some useful sites to get a good understanding of Shibboleth are:

http://www.ukfederation.org.uk/

http://shibboleth.internet2.edu/

http://shibboleth.internet2.edu/get-started.html

Virtualisation

Consider using a virtual server rather than a physical server to run your Shibboleth Identity Provider (IdP). There are commercial and open source virtualisation systems. One example is Xen which is open source. A useful link about Xen is:

http://www.xen.org/

Collaboration

Involve colleagues from the Institution’s Library or other e-Learning units at an early stage. They will probably be responsible for the user interface and will have to deal with any queries that arise from the implementation. They are also usually responsible for providing access to remote resources.

Network Requirements

Ports 80, 443, 8442 and 8443 need to be open in both directions for Shibboleth to work successfully. Port 443 provides https but any port can be used instead. However, it is often difficult to convince network people to open some other port for HTTPS traffic.

ISA Firewalls

Microsoft ISA is often used as a web proxy server. This can cause problems when HTTPS traffic is on a port other than port 443 or 563 for example the 8443 port that Shibboleth uses. On the face of it the problem is easily solved by creating new definitions for ports 8442 and 8443. For example we might create new port definitions for ports 8442 and 8443. Then it seems it is just a matter of creating ISA rules to allow traffic on these new ports through the firewall. However, this does not work. The solution is to change the tunnel port range to include the port values you wish to use. This can be done by running the following VB Script.

```
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''

' Copyright (c) Microsoft Corporation. All rights reserved.

' THIS CODE IS MADE AVAILABLE AS IS, WITHOUT WARRANTY OF ANY KIND. THE ENTIRE

' RISK OF THE USE OR THE RESULTS FROM THE USE OF THIS CODE REMAINS WITH THE

' USER. USE AND REDISTRIBUTION OF THIS CODE, WITH OR WITHOUT MODIFICATION, IS

' HEREBY PERMITTED.

''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''

''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''

' This script creates a new tunnel port range containing a single user-specified

' port to allow clients to send requests, for example, SSL requests, to that

' port.

' This script can be run from a command prompt by entering the

' following command:

'     CScript AddTPRange.vbs RangeName PortNumber

''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''

Option Explicit



' Define the constants needed.

Const Error_TypeMismatch = &HD

Const Error_AlreadyExists = &H800700B7

Const Error_OutOfRange = &H80070057
```

```
Main(WScript.Arguments)


Sub Main(args)
    If(args.Count <> 2) Then
        Usage()
    Else
       AddTPRange args(0), args(1)
    End If
End Sub


Sub AddTPRange(newRangeName, newTunnelPort)

    ' Create the root object.
    Dim root  ' The FPCLib.FPC root object
    Set root = CreateObject("FPC.Root")

    'Declare the other objects needed.
    Dim isaArray     ' An ISA Server array object
    Dim tpRanges     ' An FPCTunnelPortRanges collection
    Dim newRange     ' An FPCTunnelPortRange object
    Dim port         ' An Integer

    ' Get a reference to the array and to
    ' the collection of tunnel port ranges.
    Set isaArray = root.GetContainingArray()
    Set tpRanges = isaArray.ArrayPolicy.WebProxy.TunnelPortRanges

    ' Create a new tunnel port range.
    On Error Resume Next
    port = CDbl(newTunnelPort)
    If Err.Number = Error_TypeMismatch Then
        WScript.Echo "A number must be entered for the port to be included."
        WScript.Quit
    End If
    Err.Clear
    Set newRange = tpRanges.AddRange(newRangeName, port, port)
    If Err.Number = Error_AlreadyExists Then
       WScript.Echo "A port range with the name specified already exists."
       WScript.Quit
    ElseIf Err.Number = Error_OutOfRange Then
        WScript.Echo "The range of permissible ports is from 1 through 65535."
        WScript.Quit
    End If
    On Error GoTo 0

    ' Save the changes to the collection of tunnel port ranges
    ' with fResetRequiredServices set to True to restart the Firewall service.
    tpRanges.Save True
    WScript.Echo "Done!"
End Sub

Sub Usage()
    WScript.Echo "Usage:" & VbCrLf _
        & "  " & WScript.ScriptName & " RangeName TunnelPort" & VbCrLf _
        & "" & VbCrLf _
        & "  RangeName  - Name of the tunnel port range to be added" & VbCrLf _
        & "  TunnelPort - Port to be included in the new tunnel port range"
    WScript.Quit
End Sub
```

Further information about this and other scripts to show what ranges are in use or to delete ranges can be found in the Microsoft Technet article at:

http://technet.microsoft.com/en-us/library/cc302450.aspx

This article also includes example code which is shorter than the example shown above. However, the examples quoted in the articles do not appear to work. The one quoted above does.

Configuration

Forms Based Authentication

Many of the users of your Shibboleth Identity Provider will have limited IT experience. Consequently it is worth using forms-based authentication rather than the default Windows login box. The Shibboleth on Windows installer configures this by default but it is worth modifying the form so that it is more suitable for non IT people. For example, add links to your user registration system (if you have one) so that they can apply for an account if they don’t have one already or reset their password. If you have an online help desk system then add a link to that as well. Remember that your colleagues who are using your identity provider may not be on your campus so you need to provide them with all the facilities they need in order to do their work remotely. Instructions for modifying the login page can be found in:

http://gilbert.dev.ja.net/groups/shib/wiki/702ee/Changing_the_Look_on_the_Login_Page.html

Attribute Release Policy

The attribute release policy determines what attributes are exposed and to which sites. In most cases the release policy allows a small number of attributes to be exposed to everyone. The global attribute release policy is defined in:

C:\Program Files\Internet2\IdP\etc\arps\arp.site.xml

assuming you installed Shibboleth in C:\Program Files. Different Service Providers may require various values in the attribute eduPersonEntitlement. However, some (e.g. Eduserv) cannot accept values in eduPersonEntitlement that they do not understand. As a result the attribute release policy for these attributes has to be modified for these providers so that they do not receive the attributes they do not understand. This can be done by creating a rule that blocks specific values to specific Service Providers. For example, suppose you release a value such as AAA#ShibGlobal to EDUServ and a value such as urn:mace:dir:entitlement:common-lib-terms to another Service Provider with both values in eduPersonEntitlement so the full value of the attribute is:

AAA#ShibGlobal;urn:mace:dir:entitlement:common-lib-terms

EDUServ will treat this as an error since the string urn:mace:dir:entitlement:common-lib-terms does not match any of the attribute values that it understands. The solution is to block this value when the attribute is being exposed to Eduserv. This can be done by adding the following rule to the global Attribute Release Policy.

```
<Rule>

    <Description>Attribute Release Policy for EDUServ.</Description>

    <Target>
```

```
        <Requester>urn:mace:eduserv.org.uk:athens:federation:uk</Requester>

    </Target>

    <Attribute name="urn:mace:dir:attribute-def:eduPersonEntitlement">

        <Value release="deny">urn:mace:dir:entitlement:common-libterms</Value>

    </Attribute>

</Rule>
```

The attribute value to be blocked (which in the example is underlined) may have to be changed to suit your particular installation.

Testing

Janet Test Sites
Use the JANET test sites once Shibboleth is installed and after making any changes. Two such sites are:

https://ledi.edina.ac.uk:8885/cgi-bin/printenv

https://target.iay.org.uk/secure/printenv.cgi

Be aware that there is a slight problem with the first site in that it does not show eduPersonEntitlement even though that attribute is exposed. The second site does show that attribute correctly.

Errors and Failures
It is likely that as your Identity Provider is developed there will be things that do not work as expected. For example, it might not authenticate correctly even though the correct password is being entered or an attribute that should be released is not doing so. This can be very frustrating and the log files that Shibboleth generates on the Identity Provider may not contain enough information to resolve the problem in some circumstances. However, the log files that the Service Provider you are testing against may be. When this happens it is useful to test against one of the test sites listed above and then contact the UK Federation Help Desk with the date and time that you carried out the test. They can usually provide the relevant extract from the logs they have gathered and that can be immensely useful when diagnosing errors and failures.

Running

Log Files
The Shibboleth log files are stored in the directory:

C:\Program Files\Internet2\IdP\logs

assuming the standard location C:\Program Files was used when installing the package. The amount of information written to these files is defined in the "<Logging>" section of the file Idp.xml in C:\Program Files\Internet2\IdP\etc. The default values are Warn and Info for "ErrorLog level" and "TransactionLog" level respectively. The amount of information recorded can be increased by changing both these values to “Debug”. However, this can produce very large log files so once the issue being investigated has been resolve the values should be returned to their defaults.

Metadata File

The metadata file must be kept up to date. If it is not updated, Service Providers that have been added to the UK Federation will not be visible to people authorised by your Identity Provider. The installer automatically adds a scheduled task to download the metadata on an hourly basis but if some Service Providers are not available it is worth checking that this download is working and being done regularly.

Time Synchronization

Time synchronization is very important to Shibboleth. If the clocks on the Identity Provider and Services Provider differ by more than a few minutes, Shibboleth will be unable to authenticate users correctly. Even though people type their correct passwords they will be told that their password is incorrect. If your Shibboleth server is in a Windows Domain its clock is likely to be correct. However, if it is not and especially if it is a virtual server then some time synchronization system will be required. If you find that everyone is being told their password is wrong even though they are typing it very carefully, time synchronization is a possible cause of the problem.

Copyright

For further enquiries, please contact JANET Service Desk on service@ja.net or 0870 850 2212.

The Shibboleth on Windows Installer was a JISC funded project.

Disclaimer

This case study is provided by JANET(UK) for general information purposes only and the JNT Association cannot accept any responsibility and shall not be liable for any loss or damage which may result from reliance on the information provided in it.